IFTA®

Practical Guide to

Copyright Protection

Independent Film & Television Alliance®

IFTA® Practical Guide to Copyright Protection

Contents

Please contact the IFTA Legal Department for more information on any matters in this Guide. Your feedback, experiences and input are welcome in developing Member services that matter most to your business.

IFTA Legal Department

Susan Cleary, Vice President and General Counsel
scleary@ifta-online.org

Eric Cady, Senior Counsel
ecady@ifta-online.org

Orson Rheinfurth, Counsel & Director, IFTA Collections
orheinfurth@ifta-online.org

Marisol Figueroa, Administrative Assistant, Legal & Collections
mfigueroa@ifta-online.org

A Road Map to Protect Your Works and Enforce Your Rights

New digital platforms and distribution technology create opportunities for the independent film and television industry. Yet those same technologies also dramatically expand the ease with which a single act of infringement can rapidly spread worldwide across multiple mediums and decisively undermine revenue expectations and future financing options. The risk of theft arises well before a film or program is ready for release and should be addressed prior to production. The stakes are too high to leave to chance. Protecting the security of assets must be the responsibility of everyone in your company and of all those who touch the film or program from beginning to the end of its distribution cycle.

The IFTA© Practical Guide to Copyright Protection (Guide) is designed as a road map for independent producers, sales agents and distributors. It identifies the points of maximum exposure to security breaches and theft that damage the value of your copyrighted assets, explains what measures should be taken to minimize risks and enforce your rights, and provides references to resources that can help you create and implement a practical plan to protect your films and programs. For IFTA Members, the related Toolkit available online includes country-by-country information about local copyright and enforcement laws; templates and forms to trigger different types of protective and reporting systems; and contact information for both official and third party commercial services that provide support to the film and television industry.

The Security and Enforcement Plan

As a film or program moves from development to production to release and distribution there are many points of vulnerability that can be addressed.

> **The critical first step** is establishing basic security policies and rules for your company and its employees, vendors and distributors and to have a security and enforcement plan in place that anticipates points of exposure and appropriate response if a breach of film security occurs.

Producers and licensors and their sales agents and distributors must work together to tailor a security and enforcement plan for each film or program based on anticipated audience demand, marketing, release patterns, types of distribution platforms, and licensed windows of exclusivity. Establishing security and enforcement plans for your company[1] and identifying those responsible for implementing those standards within your company and elsewhere in the production – distribution chain is an effective way to empower participants in the industry to maintain security, disclose any breach and ensure that rapid remedial action is taken if a security breach results in proliferation of infringing copies.

[1]The U.S. National Institute of Standards and Technology established a Framework for Improving Critical Infrastructure in Cybersecurity which enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

All too frequently, companies focus on enforcement – vindicating their rights – after infringement has occurred, giving limited attention to earlier stages of the production and distribution process. **This road map is meant to encourage industry members and their business associates to give equal attention to security and prevention.** In today's digital world, it is almost impossible to "put the genie back in the bottle" once a film or program has been illegally copied and made available. Enforcement actions at best help to eliminate security gaps for the future, may delay a film's or program's proliferation online to briefly protect the legal market, and – in limited cases – may provide some financial compensation for the theft. Hence, this Guide outlines BOTH the recommended security measures to decrease the chances that an infringement will take place and enforcement steps to be taken if the worst case scenario occurs. See ***Checklist for Copyright Protection and Security at Critical Points of Vulnerability*** and ***Steps for Notifying ISPs, Payment Processors, Search Engines, and Advertisers of Copyright Infringement.***

How will Costs for the Security and Enforcement Plan be Handled?

The first questions about copyright protection are what will it cost and who will pay for security and enforcement? This Guide points you to a mix of measures, some of which are largely cost-free, such as checking on security certificates for labs and festivals, and others that may involve real out of pocket costs, such as third-party monitoring of infringements on the web.

For each recommended measure, the rights holder will need to evaluate the benefit in terms of protecting the title and how the cost of that measure will be defrayed:

- **Will the costs associated with pre-release security be absorbed as a production cost?**
- **Will security and enforcement after release be paid by the distributor as overhead or a recoupable expense?**

These are important questions that will take into account the "value" of the asset, the likelihood it will be subjected to mass infringement (often times based on the average age of the anticipated audience), the release pattern and other factors, including the bargaining power of the parties involved. Producers and distributors must decide how the overhead costs of achieving security correctly reflect the protection needs of each film or program.

Costs of copyright enforcement after release may be dealt with differently. Such costs include those associated with fingerprinting – for online monitoring – and administration of the notice and takedown process in an attempt to rid the web of infringing copies. There may also be recovery of monetary damages from civil copyright infringement actions and the producer and distributor need to agree in advance how costs of such litigation and any monetary recovery be treated. **Will recovery, whether by producer or distributor, be considered Gross Receipts after deducting the costs of the lawsuit?**[2] Though not addressed in this Guide, producers and distributors must consider whether any types of infringement can be monetized (such as through ad placement via the YouTube Content ID program), whether to allow monetization and how revenues from such monetization will be treated.

[2] See Paragraph 17.2 (Enforcement) of the IFTA International Standard Terms: Distributor will take all reasonable steps to prevent infringement or unauthorized use of the Picture in the Territory, including monitoring for infringement. Licensor at its election may independently retain its own intellectual property protection monitoring service. Licensor may participate in any copyright infringement litigation initiated by Distributor using counsel of Licensor's choice, in which case Licensor's expenses will be first reimbursed from any recovery. If Distributor declines to undertake any copyright infringement litigation, Licensor may do so at its own expense, in Licensor's or Distributor's name, with Licensor recovering all of its costs of suit, including reasonable attorney's fees, from first recoveries in such litigation, and the balance remaining being treated as Gross Receipts.

Development and Pre-Production

Security measures during development and pre-production are critical in mitigating the ongoing risks of infringement. Often, employees have access to copyrighted materials such as treatments and scripts that – if shared with the public – can damage the reaction of the public to the project or generate interest in later theft. Confidentiality and non-disclosure agreements (NDAs) should be put in place. Scripts, bibles and treatments as well as sizzle or audition reels should be inventoried, secured and shared only under tight control procedures. Because investors and sales agents have a keen interest in knowing the details of the project at these early stages, it is timely to set a strong tone and the expectation of respect for copyright security as early as possible, which later will benefit sales and distribution activities.

Production

As a project moves into physical production, and footage is generated, the risks from digital theft become more direct. **Unauthorized copies of even an incomplete production can destroy the market for the film or program and undermine relationships with distributors**. Set security is aimed at protecting both the geographic location and the materials created each day of production (production 'dailies'). These production dailies are often viewed by executives and many working remotely on the production; hence, security at this point must cover both physical and electronic sharing of sensitive files.

Security of the production dailies before and during transport to a secured laboratory is critical, as well as security of the computers or other electronic equipment used on set, so that no copies of the materials can be made without the knowledge and authority of the producer. Physical production is when the actual recording of the film or program on a tangible medium creates materials triggering copyright protection.

> Once a film or program is recorded, it should be immediately registered for copyright protection with national registration authorities such as the United States Copyright Office to identify the work and ensure that the copyright owner will enjoy the presumption of ownership and be eligible to recover statutory damages for infringement.

Facility Security: Laboratories and Post Production

Laboratories (sometimes called "digital media intermediaries") and post production houses for editing and special effects are a critical link in the production and distribution chain since copyrighted materials will be stored, mastered, edited, and reproduced in those facilities. It is prudent to understand each facility's security policies and any related certifications or assessments it may have completed. Many laboratories are "secured" facilities or "trusted partners" through site security assessment programs such as the program managed by MPAA.

These assessment programs look specifically at questions such as:

- **How will digital or physical materials be transported to the laboratory?**
- **Will the physical materials be inventoried and secured and will the digital materials be stored on a secured computer, server or 'cloud'?**
- **Who has access at the facility?**
- **Are all areas of the facility where the materials will be worked on or stored monitored by video or otherwise for security compliance?**
- **Is the facility bonded and insured against loss due to infringement of the materials?**
- **Is the rights holder a covered party under such insurance policy?**

Pre-release piracy is associated with 5% lower box office compared with piracy that occurs at release.
- Source: Carnegie Mellon University

Sales and Marketing

Markets and festivals are high pressure environments with a focus on sales and marketing of completed films and programs and those yet to be produced. Completed films or programs that are being sold will have "screeners" that are often supplied to potential buyers either on DVD or by a secured link to an electronic (encrypted) file. For the projects to be produced, pre-sales may be done based on script, key elements, and a trailer. In either case, the producer or sales agent will need to keep these materials secure to protect their other exclusive licenses already in place and preserve sales potential of the unsold territories. There may also be times when screeners are necessary for festivals, awards, censorship or ratings and security measures should be taken especially since most of these uses are pre-release. Review Best Practices for digital screeners and specifically for awards screeners. These types of security measures are critical to maintain pre-release film security, often at no or low cost.

Theatrical screenings at markets and festivals open to the public pose increased security challenges for producers and sales agents. Major festivals have agreed to accreditation by FIAPF, the International Federation of Film Producers Associations, which requires that the festival must use "stringent measures to prevent theft or illegal copyright of films" and monitors for compliance. Most festivals and markets now accommodate Digital Cinema Packages (DCPs) that are encrypted and unlocked with a unique "key" supplied to the event operators by the rights holders' laboratory. Producers and sales agents should confirm the particular event's security policies and compliance with recognized Best Practices covering how materials will be secured, whether screening attendees are tracked, whether cell phones are prohibited at the venue or the theaters are monitored for unauthorized recording, all aimed at making sure no pre-release copy can be made.

Contractual Considerations

While the producer or sales agent negotiates distribution licenses, they may have initial discussions with distributors about film security provisions which will then be incorporated into distribution agreements. Costs of security must be agreed to and the obligations of the parties must be agreed upon.

Security steps can be as basic as confirming that only security-certified labs will be used and that any sub-distribution agreement for theatrical exhibition requires certain levels of security practices in the cinemas. Or the agreement can be more complex if the distributor is obligated to share in the costs of anti-piracy monitoring, pursue infringement actions or institute other enforcement mechanisms, such as notice and take down in the licensed territory. See ***Drafting Distribution Agreements to Maximize Copyright Protection*** for an outline of the provisions of the IFTA® International Multiple Rights Distribution Agreement relating to copyright protection and enforcement.

Distribution, Pre-Release and First Release Security

Your security plan should outline measures to limit access to and secure copyrighted materials while they are in transport and being stored by distributors and sub distributors. Ideally, the security measures will give your company rapid notice of any breach of security and the ability to identify the source of a breach, allowing action to prevent any distribution or upload of infringing copies. For example, watermarking, fingerprinting and controlled access to materials or screeners are types of security tools that can identify the last custodian of a missing or duplicated copy, thus increasing the likelihood that the culprit will be stopped before infringing copies are made widely available.

There is a critical exposure window for pre-release piracy: after the completed film or program is available for delivery to distributors and prior to the first release. To address this exposure, **online monitoring for infringing copies usually begins 4-6 weeks prior to first release** to make sure there are no infringing copies or "inside" sourced copies of materials. Because so many copies are in motion and vulnerable to theft at this time, many companies declare a "temporary victory" over piracy if they can get their film or program to the date of first release to consumers without a breach of security or exclusivity.

Pre-release security measures should already have been put in place at the laboratory and at markets and festivals, and now should be observed in delivery of the materials to the distributors and sub distributors. Important security tools at this stage include the use of encryption and limited-access digital keys on digital prints, storage on secured servers, limiting access to materials for lab services and duplication, and use of bonded, specialized shipping and messenger services when transporting any physical elements. IFTA Members see ***Content Protection and Enforcement Vendor List***.

Theatrical Release and Preventing Camcording

Preservation and security of the theatrical print materials are geared toward keeping those materials secure en route to the theatrical exhibitor as well as while uploaded, stored and screened in the theaters. DCPs, and 35 or 70MM prints each call for different security measures. DCPs are secured through encryption and have a digital key that unlocks the print for upload and screening. 35 and 70MM prints must be physically secured and reels are often shipped separately so that there is no full set of prints of a completed film. Protection of the film while it is being exhibited poses separate challenges, as anonymous members of the public are given access to the work. If the first release will be theatrical, producers and distributors must discuss what measures can be adopted to strengthen security in theaters so that the film can get to the next release unscathed. What should be done in preparation for first release? What is realistic?

> Today, nearly 90% of all illegally copied movies is reported to have been initiated by use of some form of recording device (whether cell phone or camcorder) in a cinema-venue. – Source: Fight Film Theft

When establishing a security and enforcement plan, it is useful to consider the typical pattern of release for your theatrical films.

- **As an initial matter, it is critical to determine whether the recording of a film exhibited in a theater by an audience member is a violation of local law.**
- **Should your earliest theatrical releases be planned for the U.S. or another country that prohibits or makes it a criminal offense to record a film in a theater?**
- **If so, is your distributor requiring the theatrical exhibitor to operate under best practices to make sure that no filming takes place in the theater, and that any breach of the theater security policy is reported to the theater owner, then to the distributor and the producer further upstream?**
- **If there is a legal prohibition against camcording, are theater owners contractually or otherwise committed to reporting offenders to police and prosecuting?**

Theater and facility security is a detailed topic and your company's designated security supervisor should review samples of best practices such as in Australia and in North America. A joint program between the MPAA and the National Association of Theater Owners (NATO) provides incentives for theater employees to "Take Action" and report camcording activity. Even if there is no specific legal prohibition against recording in theaters, theater owners should operate under standards that prohibit recording and implement a "no use of cell phone or recording device" policy and have employees monitor for compliance. Though it is often difficult for independent producers to know what the national distributor will obligate its theatrical sub distributor to do in terms of security, these obligations should be part of your security and enforcement plan discussions and part of your consideration prior to approval of all distributors.

Television and Online Release

Many television programs with international sales appeal are high value and increasingly vulnerable to piracy because of the digital formats they are available on, as well as new release patterns including "early" and "season" release, such as the case with some Netflix series. After the initial broadcast or transmission and any "catch up period," television programming is also packaged and sold to consumers as DVDs, as downloads or streaming views or, in the case of "movie of the week" format, may also be exploited theatrically. Another concern may be "cord cheaters" who share passwords to online platforms outside the parameters of a paid subscription. **Precise windowing and the same security measures as applied to feature films should be included in a security plan for television and online exploitation.**

> The second episode of the 'Game of Thrones' fourth season broke the record for the people sharing a file simultaneously via BitTorrent with more than 193,000 individuals sharing a single copy, and roughly 1.5 million individuals downloading the episode during the first day it came online.
> – Sources: Forbes and TorrentFreak

Enforcement Options

Even under the best circumstances and utilizing strict security measures, the net result may be only that the infringement is delayed until after initial release. Producers and sales agents working diligently with their distributors to address copyright infringement know all too well that once a film or program is illegally available on the Internet, it is impossible to stop the illegal activity from spreading through the web. IFTA has consistently advocated for the adoption of strong legal frameworks and voluntary measures to obligate stakeholders – all those who produce and distribute content and those who derive economic value from the legitimate marketplace – to take action to prevent copyright infringement. In addition to legal actions against those who directly engage in infringement, voluntary measures are in place, or being developed, that encourage search engines, payment processors, ad placement agencies and others in the system to act when illegal copies or infringing activities are identified.

Under the international legal framework provided in part by the WIPO Copyright Treaty, incorporated into national law by 93 signatory countries, many countries have mandated that an ISP which transmits illegal content will be shielded as an intermediary from liability for copyright infringement if upon notification by the copyright owner the ISP removes or "takes down" the infringing digital files on their systems ("safe harbor")[3]. Thus, sending out formal requests for "take down" is a routine part of trying to control illegal copies and file-sharing. Although no country has adopted legislation for a notice, takedown and stay down framework, other remedies may be available in each country.

Courts and government authorities may be a source of relief both criminally and civilly but require that legal counsel be retained and legal precedent reviewed. For example, legal action may be taken by the rights holder for violations of civil law to secure injunctions to block further illegal activity or to recover monetary damages, or by the government for violations of criminal law.

[3] The same legal framework protects copyright holders' use of technological protection measures (TPMs) to block illegal access and copying.

Court orders may also be secured in some jurisdictions where legal precedent has been established to block illegal websites in entirety. **Courts of proper jurisdiction may also issue an order or injunction instructing the infringer or third parties to act in accordance with the Court order, sometimes ordering ISPs or search engines to take immediate actions.** Another example is that anti-camcording and other criminal laws in many countries allow a rights holder to initiate a complaint that would be investigated by government authorities and may result in criminal prosecution and penalties for the infringer. In the digital world, though, a frustrated rights holder may find that it is frequently difficult to locate the proper defendants or to determine the proper venue for legal action, and the costs of pursuing cases in civil and criminal courts are usually disproportionate to the benefits.

There are limited circumstances in which court orders may be of assistance to prevent or address mass infringement. Rights holders may pursue judicial remedies, especially in the case of pre-release piracy, such as court orders blocking access to the copyrighted asset or securing the return of the materials from the perpetrators or custodians. **In cases where reasonable evidence of illegal activity can be presented, it may be possible to obtain a court order to compel an ISP to identify customers involved in infringing activities as a preliminary to further legal action, or to compel the ISP itself to send notices to those customers.** In a handful of countries, courts also will consider orders to require ISPs to block websites that are notorious for piracy. Seeking and supporting direct governmental action such as seizures of infringing materials by customs, or the criminal arrest and prosecution of copyright infringers by police are less common but possible depending on where you seek to enforce your company's intellectual property rights.

For more information about the laws of major territories, see ***International and National Legal Frameworks for Copyright Protection and Enforcement*** and ***Country Profiles.***

ISP Notice and Takedown

Most enforcement efforts are focused on removing illegal materials from the web by notifying ISPs of the location of the infringing files on its system. ISPs are generally understood to include traditional broadband and cable providers or websites, such as YouTube, and each have designated "contacts" to which to send notifications. Even if a country does not have a statutory notice and takedown mechanism, it may have another notice program in place that can be triggered by the rights holder. These alternate programs already include systems under which ISPs are obligated to forward the notices generated by rights holders directly to subscribers, such as in Canada, or voluntary programs managed by industry stakeholders such as the Copyright Alert Program which addresses certain Peer-to-Peer (P2P) piracy in the United States and those in progress in the U.K. and Australia.

All of these efforts turn on being able to identify specific infringing files on the web, specific IP addresses or the names of participants in the infringing actions, and the date and time of the download or file-sharing. For most companies, in-house, manual web monitoring for infringing copies and notifying ISPs is an impossible undertaking, and retaining the services of companies that use technology to automate the process is a necessity. "Fingerprinting" of the content is done and then the web is scoured to find infringing copies of the file.

Infringing copies can be stored behind electronic walls in cyber lockers or shared in small segments using P2P file sharing services and/or on click and stream websites. Each of these methods requires different technological approaches to track and identify the infringing files and locations reliably and in sufficient detail for an ISP to act.

A further complexity is presented under the U.S. legal system and that of many other countries. The U.S. law – crafted in the mid-1990s – requires only that the ISP take down the specific file identified in the rights holder's notice and does not require the ISP to proactively remove any other copy or to act if the material is simply re-posted. Notices of infringement to the ISPs must be generated repeatedly and constantly (ideally, through an automated system).

Other Notifications to Search Engines, Advertisers and Payment Processors.

It is well-known that piracy is a big business for those who host notorious websites and run ongoing schemes to find and offer illegal content to consumers. **Estimates of the worldwide profits generated from advertising alone on 589 pirate websites totaled $209 million, in aggregate, for 2014**[4]. Recent focus has been on enlisting other industries with a stake in establishing a trustworthy electronic marketplace to craft voluntary programs and standards to cut off the flow of money. Payment processors (American Express, Discover, Mastercard, Paypal and Visa), advertising agencies and others now offer avenues to report piracy and to trigger investigations and action against infringing sites. Search engines may also respond to notices. For example, Google receives notices of substantially infringing websites in order to de-prioritize search engine results for sites engaged in piracy.

The City of London Police's Intellectual Property Crime Unit (PIPCU) was set up in 2013 with the intention to "dismantle and disrupt" criminal activity relating to intellectual property theft. Since then it has:

- **Suspended 2,359 Internet domain names - replacing pages with a City of London Police notice**
- **Seized more than £1.29m worth of fake goods**
- **Diverted five million visits from copyright infringing websites to a PIPCU holding page**

There also may be hotlines or other ways to directly report infringement to local Industry or governmental organizations. Some governments have organized a central point of contact between all interested parties for IP related crimes such as the United Kingdom's Police Intellectual Property Crime Unit (PIPCU) and the U.S. Department of Homeland Security's ICE unit which (respectively) allows rights holder to submit allegations electronically through an online referral and the HSI Tip Form. Rights holders are encouraged to make use of all of these programs.

[4] https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/66692a61-cd18-4c14-bede-f09ce3d84b53.pdf

'Notice and Notice', Voluntary, and Educational Programs

Since some legal frameworks may be slow to update and provide effective remedies for today's digital era, alternative approaches are being explored by cross-industry groups and tested on a voluntary basis. In the U.S., IFTA Members may participate in the Copyright Alert Program, a voluntary but limited notice program that includes the five largest U.S. ISPs and seeks to educate subscribers about the security of their computers and any infringing activity that may be occurring with a goal of decreasing P2P piracy on these systems. **The program provides for the monitoring of titles by a vendor who detects, locates and verifies instances of P2P infringement and notifies the relevant ISP.** In turn, that ISP (subject to an agreed upon limit) sends Copyright Alerts to subscribers notifying them that copyright infringement has been detected at their IP address and urges the subscriber to take measures to secure their computer. Stakeholders and ISPs within the U.K. and Australia are in the process of developing voluntary notice programs which are projected to launch at the end of 2015.

Rights Holder Notices to Infringers

Outside of the Copyright Alert Program in the U.S., **some producers and distributors are employing vendors to locate instances of infringement and send notices to ISPs that they request be passed on to the offending subscribers.** While there may be no general legal obligation on ISPs to send these notices to their subscribers whose IP addresses are captured in monitoring for illegal file sharing or downloading, some ISPs have voluntarily cooperated in sending notices from rights holders when the rights holder supplies both the notice and the IP address.

In Canada, ISPs are now required by law to pass along rights holder's notices. Whether notices are legally mandated to be forwarded by the ISP or voluntary, those notices may demand that the subscriber settle a potential infringement claim for a stated amount or the notices are a warning and ask the subscriber to seek legal sources or confirm to the producer it will do so in the future. The process does not require the ISP to disclose subscriber identifying information without a court order. Courts have periodically intervened to preclude the use of letters that overstate potential legal liability or claimed damages to justify excessive monetary demands.

Powers of Attorney

Enforcement of copyright through the judicial system requires action by a party with legal standing. Standing can be conferred by operation of law, which means that copyright owners and (usually) exclusive distributors are deemed to have the legal interest, and thus standing, to enforce and protect the copyright. A sales agent, however, does not have legal standing to pursue copyright infringement cases unless expressly granted that power by the copyright owner. This power can be granted by a legal document known as a Power of Attorney, either for a specific matter or more generally. Before granting any power of attorney or initiating any legal action or enforcement effort, the copyright owner or exclusive distributor should always determine with legal counsel the exact nature of the legal action contemplated and the risks that the action may expose the copyright owner to counterclaims, inconsistent or binding negative results, or unforeseen costs.

Working with Different Legal Frameworks and Industry Players

Each country has its own legal framework and enforcement tools. **When developing security plans that will be effective in each country of release, one must be familiar with the legal framework, industry players, and local resources and programs.** For example, if the country has an anti-camcording law and the film is being distributed theatrically, one must understand the security measures theaters can employ and the standard practices on reporting and prosecuting violations of the law. For each country, the rights holder should ask its distributor(s) what best practices are in place to make sure the day-to-day operations reflect and utilize that country's legal framework. IFTA Members may refer to the ***Country Profiles*** in the online Toolkit.

Each country also has a different framework for ISP Liability and availability of notice, or notice and takedown programs (mandated or voluntary). Piracy may be worldwide but rights holders must act locally to ensure the strongest protections are in place initially and that the most effective remedies are pursued if a breach of security occurs.

Conclusion

Due to the uniqueness of each film or program, there is no one "one size fits all" approach to best protect copyrighted assets. However, when all parties are focused on devising and implementing a security and enforcement plan that prioritizes what matters most, at a cost that reflects the value at risk, meaningful security and the mitigation of infringement can be achieved.

Checklist for Copyright Protection and Security at Critical Points of Vulnerability

All stakeholders are strongly encouraged to develop and implement a Security Plan for all phases of production and distribution. The following framework may be referred to as a starting point of discussions with your company's partners in content security as you develop a Security Plan that fits your company and each project.

Establish a Company Security Plan / Company Policies / Executive Oversight

- ✔ Perform a formal detailed evaluation of content security measures already in place.
- ✔ Designate and provide the authority and resources to a company executive to oversee the review of the Security Plan and compliance by employees, vendors and distributors.
- ✔ Review best practices and frameworks when establishing a plan for cybersecurity and content protection for your company and projects.
- ✔ Attempt to secure all contractual commitments from all third parties that they will comply with these best practices while working on the project.
- ✔ Identify points of exposure to security breaches and infringement in the production and distribution chain.
- ✔ Identify areas for improvement of security measures.
- ✔ Prioritize and implement controls to address content security risks.

Establish a Security Plan for your company and employees.

- **Require all employees to sign a confidentiality and/or non-disclosure agreement regarding proprietary content.**
- **Require all employees to return all company owned content in their possession upon termination.**
- **Maintain electronic log of all access to servers and production networks containing pre-release content.**
- **Delete employee accounts and/or block employee access to company networks upon termination.**

- ✔ Coordinate with producers, licensors, sales agents, vendors and distributors to tailor a Security and Enforcement Plan for each film or television program based on marketing, release patterns, types of distribution platforms, and licensed windows of exclusivity.

During Development, Production and Post-Production

- ✔ Consider engaging professional services that protect and secure physical and digital materials. IFTA Members see ***Copyright Protection and Enforcement Vendor List.***
- ✔ Contractually require producers, sales agents, distributors, labs, vendors and employees to have in place and at all times abide by security measures that guard against piracy during the entire chain of production and distribution. See sample contractual language in ***Drafting Distribution Agreements to Maximize Copyright Protection.***

Restrict and secure access to all sets, locations, production facilities, and all other areas where content is handled.

- **Restrict access to only those individuals required to be there as part of their job function.**
- **Require all visitors to check-in and maintain a detailed visitors' log.**
- **Secure all entry/exit points.**
- **Install security video recorders to record all entry/exit points and restricted areas.**
- **Conduct searches, as permitted by local law, of personnel and prohibit entering/exiting with digital recording devices, including Mobile Devices.**

- ✔ Inventory and secure computers, cameras or other electronic equipment used to view or store content.
- ✔ Inventory and secure copies of scripts and other copyrightable materials.
- ✔ Utilize secure or encrypted delivery and storage for production dailies.
- ✔ Identify content with digital identifiers or metadata. Register and affix an International Standard Audio-visual Number (ISAN), Entertainment Identifier Registry (EIDR) or similar unique identifier to the content with descriptive metadata.
- ✔ Consider using Playback Control Watermarking on theatrical prints and DCPs.

Develop and follow best practices for laboratory security and delivery.

- **Use "trusted" and bonded laboratories that employ controls and operate under the MPAA's Best Practices.**
- **Use *IFTA® International Laboratory Access Letter.***
- **Conduct background and reference checks on laboratories.**
- **Encrypt all materials leaving the laboratory.**
- **Use specialized, bonded messenger services for physical delivery of any materials.**
- **Use encrypted and secure networks for delivery of any digital materials.**
- **Encrypt all content and track and log all shipments.**

Secure network infrastructure.

- **Use firewalls where applicable.**
- **Maintain separate network for production and/or content.**
- **Restrict access to production network.**
- **Block production network and/or devices used to process or store digital content from connecting to the Internet.**
- **Secure all backups of content and devices.**

- ✔ Register copyrights and record exclusive rights to content with appropriate government authorities, such as the United States Copyright Office.
- ✔ IFTA Members use ***IFTA® Certification*** and ***Rights Verification Programs.***

During Sales and Marketing Activities, Pre-Release

- ✔ Draft Distribution Agreements to maximize copyright protection including requiring use of DRM and encryption. See ***Drafting Distribution Agreements to Maximize Copyright Protection.***
- ✔ Consider requiring distributors to monitor for online piracy and participate in voluntary or government graduated response or other programs, if available.
- ✔ Encrypt and store all digital copies on secured and encrypted servers or computers.

Establish security policies for all digital screeners, including screeners used for awards.

- **Require written approval to access all digital screeners.**
- **Maintain a log and inventory of those with access to screeners.**
- **Code, serialize or otherwise forensically watermark (to enable tracking) all materials.**
- **Require all users to destroy screeners after viewing.**
- **Destroy and/or delete all unused or returned screeners.**

- ✔ Establish a "no cell phone or recording device" policy for all pre-release screenings.
- ✔ Use camcorder detection equipment at all festival screenings open to the public.
- ✔ Confirm security practices for exhibition at festivals and ensure compliance with FIAPF security requirements.
- ✔ Use Forensic Watermarking and/or Fingerprinting on all screeners in order to identify and locate infringing copies or sources of security breaches. Use an encrypted DCP at pre-or initial release screenings.
- ✔ Physically lock up all screeners, especially at busy markets.

If a trusted digital screening platform is used to make screeners available, then use secured links for screeners and require verification of access.

- **Assign unique credentials to all users.**
- **Send digital keys separately from encrypted content.**

- ✔ Use security text on trailers and screeners with specific guidelines for all recipients, including notification that each copy (master tape/digital file) may be tracked and sourced to the recipient.
- ✔ For content that generates strong pre-release interest or publicity, consider engaging the services of an Investigative company vendor to monitor online chatrooms/release groups and to intercept pre-release content leaks.
- ✔ Use *IFTA® International Multiple Rights Distribution Agreement* or *Deal Memo* which contains copyright protection provisions.

During Distribution and Release

- ✔ Consider retaining online monitoring services prior to first release to police the web for any content security breach and to send take down notifications. IFTA Members may consult the ***Copyright Protection and Enforcement Vendor List.***
- ✔ IFTA Members may participate in the U.S. Copyright Alert Program.
- ✔ Allow only secure access to materials deposited at laboratories.
- ✔ Require distributors to store all digital materials on secure servers.
- ✔ Require distributors to exhibit in theaters that employ security Best Practices.

Develop and implement best practices to secure materials and prevent camcording in theaters.

- **Consider Forensic Watermarking theatrical prints.**
- **Utilize government warnings and seals when available, such as the U.S. FBI warning.**
- **Supply digital keys separate from DCPs and ship theatrical print reels separatley.**
- **Consider day-and-date theatrical release, if possible.**
- **Upon expiration of license, always obtain certificate of destruction of all materials.**
- **Encourage or require theaters and employees to Take Action and report instances of camcording to law enforcement authorities even where specific anti-camcording laws are not in place.**

Develop and implement best practices for video / optical disc security.

- Use only bonded facilities with security policies to master and press discs.
- Confirm optical disc plants use SID Codes to identify the pressing plant.
- Consider using Digital Rights Management.
- Consider using anti-rip protection.
- Consider using Playback Control Watermarking and Fingerprinting.

- ✔ Develop and implement best practices for cable / broadcast / satellite security.
- ✔ Be aware of satellite footprints and broadcast overspill.

Develop and implement best practices for security for online exploitation.

- Use *IFTA® International Multiple Rights Distribution Agreement* (including the Internet and ClosedNet Exploitation Obligations at Paragraph 13.5 of the IFTA® International Standard Terms).
- Use "trusted" vendors for all digital intermediary and laboratory service providers.
- Make sure that online platforms authenticate subscribers and address "cord cheaters".
- Use Digital Rights Management, Fingerprinting and/or geofiltering technology.
- Consider using Internet monitoring, notice and takedown services. IFTA Members may consult the *Copyright Protection and Enforcement Vendor List.*
- Require blocked input/output capabilities based on a defined standard applied on all systems that handle or store digital content.
- Implement encryption techniques and require authentication on all hard drives and USB devices used to transport content.

Notify and report criminal activity.

- **If there is a major security breach pre-release, report immediately to local authorities such as PIPCU in the UK and the IPR Center or Customs in the U.S. of infringing copies and determine the source and prevent the upload.**
- **Report or require others to report criminal activities to local law enforcement authorities and industry organizations such as the NATO and Industry Trust UK or other government notifications programs such as the P2P notification system in France administered by HADOPI.**

- ✔ Retain private investigative services to conduct monitoring of chatrooms and cyberlockers in order to determine if there are pre-release copies available for sale or share.
- ✔ Notify ISPs of infringement taking place on their system and demand immediate removal of the infringing copies.
- ✔ Notify Payment Processors when their services are used to process payments in connection with the illegal distribution of content.
- ✔ Notify advertisers and their Ad Brokers if their advertisements are displayed with illegal copies of your content.
- ✔ Notify Search Engines of websites that are engaged in illegal activity so that the address of the infringing website may be de-prioritized in search results. Notify Search Engines to remove URLs of infringing files that appear high in search results for title of content or search queries such as “Watch (Title of Content)”.
- ✔ Notify App Stores of apps they offer for sale that are used for infringing activity.
- ✔ IFTA Members may use the Toolkit’s Notification Forms.
- ✔ Consider other legal remedies to disrupt or prevent infringing activity.
- ✔ Discuss enforcement options and costs with distributors.
- ✔ Empower distributor or sales agent to report and enforce copyright.
- ✔ Consider retaining local counsel for civil enforcement of copyright.
- ✔ Consider filing a legal action to obtain an injunction to disrupt piracy, such as through Court ordered website blocking.

International and National Legal Frameworks for Copyright Protection and Enforcement

	Berne Convention	WIPO Copyright Treaty (WCT)	TRIPS	ISP Notice System	Court Ordered Website* - Blocking Injunctions	Anti - Camcord Law
Australia	✓	✓	✓	✓	✓	✓
Belgium	✓	✓	✓	✓	✓	
Brazil	✓		✓	✓		
Canada	✓	✓	✓	✓		✓
Chile	✓	✓	✓	✓		
China	✓	✓	✓	✓		
Denmark	✓	✓	✓	✓	✓	
France	✓	✓	✓	✓	✓	
Germany	✓	✓	✓	✓	✓	
Greece	✓	✓	✓	✓	✓	
Hong Kong			✓			✓
India	✓		✓	✓		
Ireland	✓	✓	✓	✓	✓	
Italy	✓	✓	✓	✓	✓	✓
Japan	✓	✓	✓	✓		✓
Mexico	✓	✓	✓			
Netherlands	✓	✓	✓	✓	✓	
New Zealand	✓		✓	✓		
Poland	✓	✓	✓	✓		
Republic of Korea	✓	✓	✓	✓	✓	✓
Russian Federation	✓	✓	✓	✓	✓	
Spain	✓	✓	✓	✓	✓	✓
Sweden	✓	✓	✓	✓	✓	
Switzerland	✓	✓	✓	✓		
United Kingdom	✓	✓	✓	✓	✓	
United States of America	✓	✓	✓	✓		✓

*Site blocking refers to an ISP blocking its subscribers' access to a certain website. Although site blocking may not be available in certain territories, it may be possible to get other forms of injunctive relief against infringing websites.

International and National Legal Frameworks for Copyright Protection and Enforcement

Copyright protection and enforcement options against copyright infringement in a particular country depend on the national intellectual property laws of each country.

The basic level of protection and enforcement mechanisms for audiovisual works are established in local law in many countries and further harmonized through international treaties. The key treaties affecting copyright include:

- **The Berne Convention for the Protection of Literary and Artistic Works (Berne)**
- **WIPO Copyright Treaty (WCT)**
- **Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)**

These treaties – adopted into signatory partners' local laws -- are the backbone of an international legal framework for copyright and establish basic principles such as the legal presumption of ownership and exclusive use (subject to exceptions and limitations) of the copyrighted work. They also require adoption of laws providing legal remedies to address infringement, to deter circumvention of technological measures intended to protect the owner against unauthorized uses and to provide criminal liability for certain types of piracy.

Other bilateral and multilateral agreements may establish higher levels of protection. These would include treaties such as the U.S.-Korea Free Trade Agreement and the specific Directives on Copyright and on E-Commerce adopted pursuant to the Treaty on the European Union.

The legal framework for copyright of each country may expressly require additional protections or enforcement mechanisms and be based on that country's individual attempt to address online or physical copyright infringement. National laws such as in the United States may extend civil liability for intermediaries such as ISPs and websites who knowingly allow infringement to occur on their systems and establish a safe harbor for those ISPs which take down the infringing file after proper notification by the rights holder. Other countries such as Canada may not obligate the ISP to take down infringing files but compel its cooperation in sending a notification from the rights holder to its subscribers engaged in infringing activity.

Countries may also establish criminal liability for those who repeatedly violate copyright laws, engage in commercial-scale infringement or violate specific laws prohibiting the recording of a film being exhibited in a theater. Court decisions, orders or injunctions in that particular jurisdiction providing relief to copyright owners are also an important part of the legal framework of each country. Judges have a wide range of remedies they

can fashion for rights holders to disrupt or stop specific infringements including ordering the return of stolen copyrighted materials, ISPs to turn over the names and addresses of those engage in infringing activity on their systems, a search engine to de-list an infringing website, ISPs to block access to an infringing website, or an infringing website to cease all illegal activity in that jurisdiction.

Despite a well adopted international legal framework, there still is not one "standard" set of laws and court decisions regarding notice process (if any), website-blocking and other remedies so rights holders will need to determine with their distributors the most effective mechanisms to utilize in each country. Much enforcement is focused on legal systems which provide for the ability to notify ISPs of infringing files on their systems so that the infringing file is removed from the system or the subscriber engaging in illegal activity can be contacted in order to stop.

The following is a brief description of the major international treaties and conventions that affect copyright[1]:

The Berne Convention

The Berne Convention for the Protection of Literary and Artistic Works was adopted in 1886 (the Berne Convention) and focused international attention on copyright issues. As of May 2015, 168 countries are members of the Berne Convention[2].

The Berne Convention rests on the three following basic principles:

1. **National Treatment** foreign works must be given the same copyright protection in each member country as the member country grants to works of its own nationals;
2. **Automatic Protection** the protection must not be conditioned upon compliance with any formality, such as affixation of a copyright symbol ("©") or registration; and
3. **Independence of Protection** the protection must be independent of the copyright protection afforded in the foreign work's country of origin.

[1] The selected treaties and conventions are not an exhaustive list of all international agreements that affect intellectual property rights, but rather a list of agreements pertinent to the copyright interests of the independent film and television industry. The information provided herein is merely a summary of basic principles. Please refer to the full text of the international agreements for a full understanding of all of the relevant provisions.

[2] For a list of the contracting member countries to the Berne Convention visit: http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15.

The Berne Convention also provides minimum standards of protection to copyrighted works, including the specific rights to be protected and the duration of protection (50 years after the death of the author), though signatory countries are free to provide protections that exceed the Berne Convention standards as is now the case in many countries. Further, it requires signatory countries to recognize the author's exclusive rights of authorization, which include among others the right to broadcast, the right to make reproductions and the right to use the work as a basis for an audiovisual work.

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)

TRIPS establishes international minimum standards for intellectual property protection both in its substantive and enforcement provisions. TRIPS also provides an important link between intellectual property rights protection and the trade portions of the Uruguay Round agreements (establishing the World Trade Organization (WTO)) and is Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in 1994.

The TRIPS Agreement incorporates by reference the 1971 Berne Convention and sets forth the obligations of WTO members to adequately and effectively enforce intellectual property rights, including copyright (Section III of TRIPS, Articles 41-61). As of May 2015, 161 countries are members of the TRIPS[3].

WIPO Copyright Treaty

The WIPO Copyright Treaty (WCT) was adopted on December 20,1996 and prohibits the circumvention of technological measures used to protect copyrighted works and prevents tampering with rights management information in the works[4]. It also provides legal remedies against the removal or tampering with copyright management information, more commonly referred to as "digital rights management" (DRM). While the WCT (adopted 2 years prior to the U.S. DMCA) does not expressly provide for the specific remedy of notice and takedown with the commensurate safe harbor for ISPs that comply, it did require that all countries that enforcement procedures are available to permit effective action against infringement including the expeditious remedies to prevent infringements.

Article 14 of WCT Provisions on Enforcement of Rights Provide:

1. Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

2. Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.

[3] For a list of the contracting member countries to TRIPS visit: https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[4] "Circumvention" means the disabling of any copy-protect mechanisms, or any activity that makes circumvention possible. "Copyright management information" is more commonly referred to as "digital rights management" (DRM).

Implementation of Treaty Obligations

United States

The Digital Millennium Copyright Act ("DMCA")[5] implemented the WIPO Copyright Treaty in the United States and was adopted in 1998. The U.S. DMCA expanded existing Copyright Law in the United States and for the first time established a notice and takedown system that allowed Internet Service Providers ("ISPs") to take "a Safe Harbor" from liability for copyright infringement if the rights holders meet specific notice requirements and the ISP complies with proper notice by taking down infringing files on their systems.

The DMCA puts the initial burden to discover the infringing material and notify the ISP of the infringing file on the rights holder so that the ISPs have "actual knowledge" and their duty to "takedown" is triggered. The ISP is then required to takedown that specific infringing file which was the subject of the notification. However, the alleged infringer may send the ISP a counter notice of non-infringement, in which case the ISP is required to replace the files pending formal legal action by the rights holder. Since there is no proactive duty for the ISPs to prevent the upload of that same or other infringing files of that same copyrighted work onto its system unless again notified of infringing files, infringing files are taken down only to reappear from the same or another uploader. Even with a clear takedown law, rights holders are trapped in an endless cycle of monitoring the vast Internet and sending notices of infringing files to ISPs.

Proper ISP Notice Under U.S. DMCA

Section 512(c)(3) of the United States Copyright Act, the written notice of alleged infringement submitted to an ISP must contain substantially all of the following:

a. **A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.**

b. **Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.**

c. **Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.**

d. **Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.**

e. **A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the rights holder, its agent, or the law.**

f. **A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.**

[5] Visit the US Copyright Office website (http://www.copyright.gov/title17) for the full text of US Copyright laws, including the DMCA.

IFTA Members see the ***Copyright Infringement Notification Forms*** that comply with U.S. Law and may be used as a sample infringement notification outside the U.S. However, rights holders are advised to consult local counsel to establish what is required under local copyright law.

In April 2015, the U.S. Department of Commerce's Internet Policy Task Force (IPTF) released a document titled, "DMCA Notice-and-Takedown Processes: List of Good, Bad, and Situational Practices" designed to improve the DMCA's notice and takedown system. The document was developed as part of a multi-stakeholder forum aimed at identifying best practices and/or produce voluntary agreements for improving the operation of the current DMCA notice and takedown system. The Working Group did not contemplate systemic improvements that would include a notice, takedown and stay down system because there is no basis in current Law.

The European Union Directives[6]

The European Union has enacted laws to limit copyright infringement liability of ISPs and to implement the WCT[7]. In 2000, the European Council adopted the Directive 2000/31/EC, commonly known as the **Electronic Commerce (E-Commerce) Directive**, which established the principle of "notice and takedown." However, unlike the DMCA, the E-Commerce Directive does not codify a specific notice and takedown procedure for Member States, so notice and takedown laws may vary across the EU.

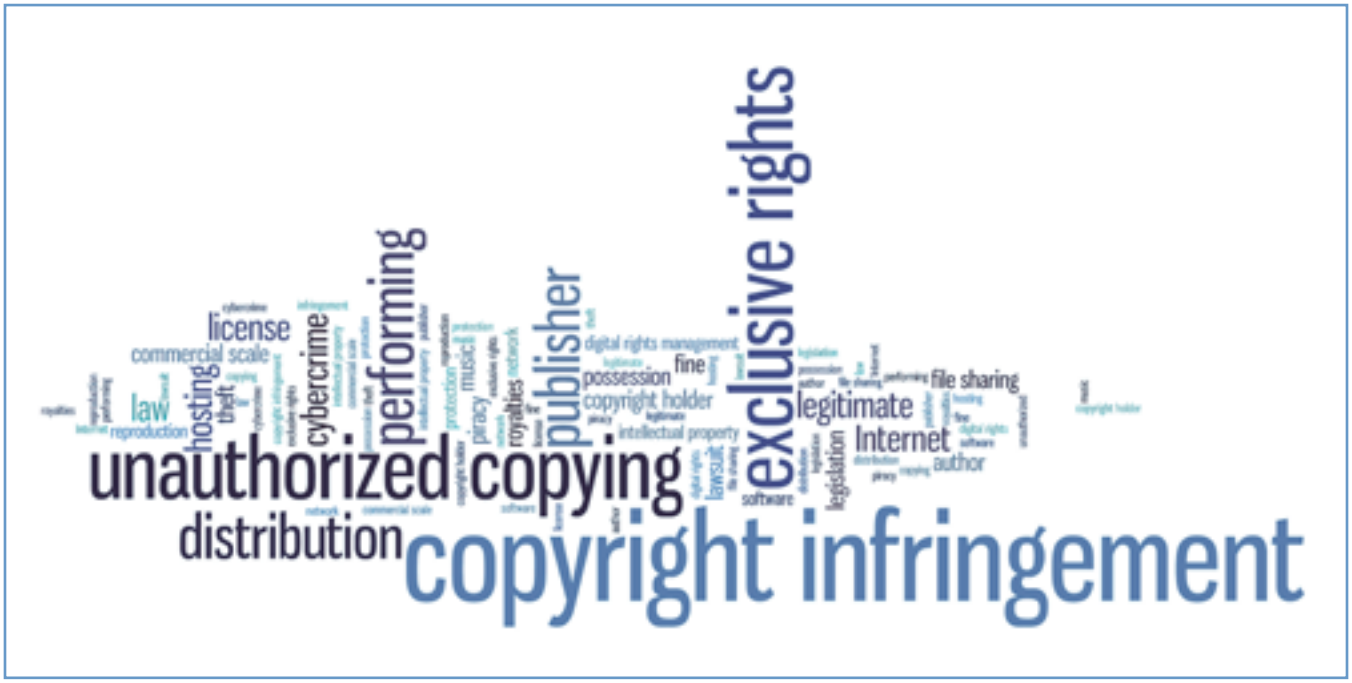
The E-Commerce Directive deals with many issues of electronic commerce including electronic contracts, spam and dispute resolution. It mandates, in part, that EU Member States exempt ISPs from copyright infringement liability where:

1. **The ISP acts as a mere conduit for the offending transmission**
2. **The ISP is merely "caching," i.e., temporarily storing the information; or**
3. **The ISP is a "host," storing the information of its customers. The ISP loses immunity in the latter two situations once it has knowledge that the information is illegal, unless it promptly removes the information upon gaining such knowledge.**
4. **Article 14 then provides that upon notification the ISP must expeditiously remove or disable access to the infringing material.**

[6] The European Council approved the WIPO Copyright Treaty on March 16, 2000.
[7] The European Union Directives that largely cover the subject matter of the WIPO Copyright Treaty are Directive 91/250/EC, Directive 96/9/EC and Directive 2001/29/EC. For text of EU Directives and more information on EU law, visit the EU law website at: http://eur-lex.europa.eu/en/index.htm.

In 2001, the European Council adopted Directive 2001/29/EC, commonly known as the **EU Copyright Directive**, which provides that Member States must provide appropriate legal protection against the circumvention of any technological measures used to safeguard copyrights and ensure that rights holders can apply for an injunction against Internet intermediaries whose services are used by a third party to infringe a copyright [8].

In 2004, the European Council adopted Directive 2004/48/EC commonly known as the **Enforcement Directive**, which provides for civil remedies to infringement only and does not have provisions for criminal offenses and requires Member States to ensure that measures necessary for the enforcement of intellectual property rights shall not be unnecessarily complicated or costly. The Enforcement Directive was also not designed with online enforcement in mind but may be considered effective to address enforcement for all types of infringement.



See ***Steps for Notifying ISPs, Payment Processors, Search Engines, and Advertisers of Copyright Infringement***.
IFTA Members, see ***Country Profiles*** in the online Toolkit.

[8] In 2014, the Court of Justice of the European Union held that ISPs can be ordered to block access by customers to websites making available infringing content and ISPs are free to choose the measures they use provided those measures target the infringing content and do not unjustly interfere with the users' right to freedom of information *(See UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft).*

Steps for Notifying ISPs, Payment Processors, Search Engines, and Advertisers of Copyright Infringement

Even though you have employed security measures to protect your copyrighted assets, online piracy may occur. Some countries such as the U.S. have established a legal framework requiring ISPs to remove infringing materials from their systems when notified by the rights holder. If the ISP, upon notification, removes the material in the time period specified by law they usually enjoy a "safe harbor" from liability for copyright infringement. Some countries do not require that an ISP remove infringing content without a court order but do require the ISP to notify (or pass along the notice from the rights holder) to the subscriber engaging in infringing activity.

In countries where no duty is imposed on ISPs, the rights holder should still notify the infringing activity because it may violate the ISP's terms of service with its subscriber. Some countries like the United States have a statutory notice and takedown framework, and a separate voluntary alert program in which IFTA Members may participate. It is difficult and time consuming, and often costly with minimal positive results, to monitor for all instances of infringement. **Rights holders may consider consider using a vendor who will fingerprint content, monitor the web for infringing copies and automate the notice sending process for specific films or programs.**

IFTA Members may refer to the online Toolkit available for their use. The Toolkit contains notification Forms and more information on companies that offer services to automate the monitoring and notice process. See the ***Copyright Protection and Enforcement Vendor List.***

If your company chooses to send infringement notices, below are some steps to help in the process:

Step 1 Identify the online location of the infringing material.

- **Identify the IP address and URL of the infringing website by using a website geographic location tool such as** www.site24x7.com/find-website-location.html**.**

Step 2 Find the contact details of the infringing website.

- **Determine the contact details and proprietor of the infringing website.**
- **Determine if the website has any redirects to other websites by using** www.webconfs.com/redirect-check.php. **If so, locate all URLs and contact information of the redirected domain.**
- **Check and compare the contact details using** WHOIS **search and** www.dnsstuff.com**.**

Helpful Tips:
Online tracking tools, such as WHOIS and DNSstuff can be used to find information, such as the domain name proprietor(s), or the domain name registrar or registering agency (if any). The search results will often vary depending on the information contained in the relevant databases. An infringing website may register its domain name through a registering agency which are used to intentionally conceal the domain name proprietor's identity and contact information. However, the tracking tools provide a solid basis to begin the search for the parties involved with the online content theft, or hosting, of a protected film or program.

The following contact information will be helpful in sending a takedown notice:

- **Registrant Name**
- **Address**
- **Phone Numbers**
- **Email Address**
- **Domain booking date**
- **Domain expiration date**
- **Name Server**
- **IP Address of infringing website and file**

Step 3 Determine whether the offending website provides "terms of use" or procedures to follow in the event of an infringement on the website.

- **Check the infringing website for any information regarding how to report copyright infringement.**

Step 4 Determine the applicable law(s) and remedies available in the country where the infringing website is located.

See ***International and National Legal Frameworks for Copyright Protection and Enforcement*** for more information on applicable laws and remedies.

For additional information on the legal framework of major territories, IFTA Members should review the ***Country Profiles*** available exclusively to them in the online Toolkit at www.ifta-online.org

Step 5 Send notice of the infringement.

Helpful Tips:
Copyright infringement notification requirements of the U.S. DMCA §512 requires that rights holders provide certain information to ISPs. See ***International and National Legal Frameworks***, IFTA Members see ***ISP Notification Form*** in the Toolkit.

Step 6 Determine whether any major payment processors (e.g., American Express, Discover, MasterCard, PayPal and Visa) are used in connection with the infringing website.

- **Check infringing website for any use of payment processor logos.**

Helpful Tips:

In response to a process facilitated by the U.S. Intellectual Property Enforcement Coordinator, five major U.S. payment processors (American Express, Discover, MasterCard, PayPal and Visa) signed on to a voluntary agreement to respond to reports from rights holders that certain vendor websites are engaged in the sale of pirated or counterfeit goods and established the Best Practice for Voluntary Measures in Addressing the Sale of Counterfeits on the Internet. Specifically, upon proper notification by a rights holder that a vendor website distributes illegal content or products, the participating payment processor will take action to investigate and in certain circumstances cut-off the financial services to the infringing website.

Under the voluntary agreement, the participating payment processors each will maintain a website containing a clearly identifiable complaint mechanism for rights holders, including a point of contact for the payment processor, and policies prohibiting the sale of illegitimate products using the payment processors' services. However, the specific procedures employed by each participating payment processor may vary.

IFTA Members may use the ***IFTA Payment Processors Notificaton Form*** in the Toolkit to report infringing sites that market to U.S. users and use PayPal, Visa, MasterCard, Discover or American Express to process payments.

Step 7 Notify search engines to limit visibility of an infringing website.

Helpful Tips:

Search engines may accept notices of websites featuring infringing content.

The Notice is similar to a DMCA Notice and requests that the search engine de-list the infringing website. IFTA Members see the Toolkit's ***Sample Notice to Search Engines for Deprioritization of Search Results***.

Google has stated that it factors the number of valid copyright removal notices received for any given site as one signal taken into account when ranking search results. In theory, websites with high numbers of DMCA removal notices may appear lower in the Google search results, in an effort to discourage infringement and facilitate use of legitimate sources of content. For more information, see Google Report.

Step 8 Determine whether the infringing website is supported by advertisements.

- **Check the infringing website for any advertisements.**
- **Determine the source of the advertisements.**
- **Take a screenshot of the infringing website displaying the advertisement.**

Helpful Tips:
Send written notice to the ad companies urging them to remove their ads from the infringing website and prevent further dissemination of their ads on infringing websites. IFTA Members see Toolkit's ***Sample Online Copyright Infringement Notification to Advertiser or Ad Broker.***

The Association of National Advertisers (ANA) and the American Association of Advertising Agencies (4A's) have issued a Statement of Best Practices to Address Online Piracy and Counterfeiting, which has also been supported by the Interactive Advertising Bureau (IAB). These best practices serve as a means to discourage advertisers from providing financial support to, or otherwise legitimizing, Internet sites whose primary and apparent purpose is online copyright infringement.

The Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting provides guidelines for Ad Networks to follow, including maintaining and posting their own internal procedures for accepting and processing valid, reasonable, and sufficiently detailed notices from rights holders regarding websites alleged to be principally dedicated to piracy, to prevent these websites from participating in the Ad Network's advertising programs.

The Trustworthy Accountability Group (TAG) has established the Brand Integrity Program Against Piracy to help address issues of malware, fraud, piracy, and lack of transparency, and reduce the air of legitimacy given to websites carrying counterfeit products, including pirated films and television programing, by removing advertisements of legitimate brands from those websites. The program allows advertisers to use technology companies which have been validated as Digital Advertising Assurance Providers (DAAPs), to identify websites and properties that don't meet that advertiser's standards.

Step 9 Special Circumstances

YouTube

Helpful Tip:
Send a copyright infringement notification pursuant to the U.S. Digital Millennium Copyright Act ("DMCA") to the YouTube designated Copyright Agent. The contact is: **Shadie Farazian,** Copyright Agent 901 Cherry Ave., San Bruno, CA 94066 **Email** copyright@youtube.com **Fax** 650-872-8513. For Instructions, click here. To submit a copyright infringement notification via YouTube's online webform, click here.

In addition, YouTube operates a Content ID Program and Content Verification Program. Although the criteria to participate in these programs is not clear, through the Content ID Program, rights holders may request automatic identification of unauthorized copyrighted material appearing on the website and establish parameters in response that include data collection, monetization or removal of the infringing material. The Content Verification Program is designed for rights holders to issue multiple removal requests.

Peer-to-Peer Networks

Peer-to-Peer (P2P) networks consist of networks of linked computers whereby users are able to upload and share pieces of a file to other users who then download those pieces and use software to compile the pieces into a complete file. Since it is difficult to pinpoint the location of the files stored on individual computers, issuing takedown notices for this type of infringement can become time-consuming and often cost-prohibitive. Consider retaining a content protection vendor that monitors for this type of infringement and sends automated takedown notices. IFTA® Members also can participate in the voluntary U.S. Copyright Alert Program.

Drafting Distribution Agreements to Maximize Copyright Protection

Several provisions of the IFTA® Model International Licensing Agreement ("MILA") maximize intellectual property protection and should be included in the Distribution Agreement by the Licensor. For example:

> ***Copyright Notice Requirements*** *Distributor will include on each Copy of the Picture distributed under its authority any copyright notice, trademark designation, anti-piracy warning and rights management information included on any Delivery Materials or otherwise supplied by Licensor.*[1]

> ***Enforcement*** *Distributor will take all reasonable steps to prevent infringement or unauthorized use of the Picture in the Territory, including monitoring for infringement. Licensor at its election may independently retain its own intellectual property protection monitoring service. Licensor may participate in any copyright infringement litigation initiated by Distributor using counsel of Licensor's choice, in which case Licensor's expenses will be first reimbursed from any recovery. If Distributor declines to undertake any copyright infringement litigation, Licensor may do so at its own expense, in Licensor's or Distributor's name, with Licensor recovering all of its costs of suit, including reasonable attorney's fees, from first recoveries in such litigation, and the balance remaining being treated as Gross Receipts.*[2]

> ***New Technology*** *If during the Term new technology in general commercial use in the Territory inhibits the unauthorized duplication, reception, access, downloading or exploitation of the Picture or its Copies, then Distributor will use such technology in a reasonable manner in exploiting the Licensed Rights in the Picture. Distributor may deduct the reasonable cost of so doing as a Recoupable Cost after obtaining prior Notice of Licensor's approval.*[3]

> ***No Warranty Against Infringement*** *The Parties acknowledge that it is in their mutual interest to prevent infringement and unauthorized distribution of the Picture in the Territory. Distributor has also taken all necessary steps to inform itself of any infringement of the Picture in the Territory before executing this Agreement. No infringement or unauthorized distribution of the Picture, whether before or after the Effective Date, will allow Distributor to terminate this Agreement, reduce any amounts due to Licensor or alter the terms of exploitation including any Holdbacks. Licensor will cooperate with Distributor to prevent or remedy any such act of infringement or unauthorized distribution of the Picture.*[4]

[1] IFTA International Multiple Rights Distribution Agreement, Paragraph 17.1.
[2] IFTA International Multiple Rights Distribution Agreement, Paragraph 17.2
[3] IFTA International Multiple Rights Distribution Agreement, Paragraph 17.3.
[4] IFTA International Multiple Rights Distribution Agreement, Paragraph 17.4.

> ***Electronic Delivery*** *The Licensor will deliver the applicable Delivery Materials to Distributor by electronic transmission over the Internet or comparable service consistent with available materials and Distributor's equipment. In so doing, Licensor may require Distributor to obtain and use reasonable and commercially available digital rights management software and intellectual property protection before making any electronic delivery.*[5]

Although not specifically mentioned in the MILA, consider discussing with your Distributor the benefits and costs of participating in any voluntary or government programs available in the territory to combat piracy. Also consider an MFN provision to obtain the same protections offered to the Major U.S.-based studios.

Convey a Power of Attorney to the Distributor or a Sales Agent

Distributors should be obligated to take all reasonable steps to prevent copyright theft of the Picture in the Territory, including monitoring for infringement. However, the terms of the Distribution Agreement alone may not be sufficient to enable Distributors to initiate legal proceedings or to file criminal complaints without more specific authorization. Under national copyright law, an exclusive Distributor may have legal standing to take such actions; a non-exclusive Distributor or a Sales Agent likely would not have legal standing to do so. Authority to take such actions may be conveyed through a valid and enforceable Power of Attorney (POA) and such POA may be provided either within the terms of the Distribution Agreement or in a stand-alone document executed in connection with a specific set of circumstances. Companies are urged to consult with legal counsel to ensure that any form of POA they use is valid for that jurisdiction and that it contains clear provisions as to the scope of the authority that the Licensor is granting. See ***International and National Legal Frameworks for Copyright Protection and Enforcement***.

Uses that May Not be Considered Copyright Infringement

When addressing situations involving distribution not covered by an existing grant of rights, it is important to identify if the exploitation is an unauthorized use OR an act of copyright infringement by another party. **When the exploitation is an unauthorized use by an existing Distributor and/or a breach of the Distribution Agreement**[6]**, the Licensor may find a solution by working with its Distributor to resolve the situation and usually must rely on the contract for remedies rather than intellectual property laws.**

[5] IFTA International Multiple Rights Distribution Agreement, Paragraph 12.4.5.

[6] Paragraph 16 of the IFTA International Standard Terms covers Termination, Cancellation and Default. IFTA Members may refer to the online Toolkit for a Sample Notice of Default and Demand to Cure Letter and Sample Notice of Cancellation Letter.

Broadcast Overspill

Broadcast overspill by a Distributor is the inadvertent, incidental broadcast into an adjacent territory. The Licensor should state in the Distribution Agreement that it does not grant exclusivity protection against reception in the Territory of a broadcast (or authorized simulcast) or Simultaneous Retransmission of the film or program originating outside the Territory, whether received by terrestrial, cable or satellite or any other means (including but not limited to Internet and/or a Closed Network). Paragraphs 3.4, 3.5 and 6.5 of the MILA collectively provide that Licensor should agree that during the License Period for any PayPerView, Pay TV or Free TV Licensed Rights it will not broadcast or authorize others to broadcast the film or program in any Authorized Language within the region where the broadcast is intended for primary reception within the Territory, but such agreement does not apply to the original, un-subtitled English language version of the film or program even if English is an Authorized Language, unless English is an official language in the Territory.

Breaching a Holdback Period

Where a license contains specific provisions requiring the Distributor to holdback the exploitation of specified media until particular time periods have expired and the Distributor fails to honor such holdbacks, this distribution (or broadcast) usually is not considered infringement, but rather may be considered a breach of the Distribution Agreement. The Licensor should prohibit the Distributor from exploiting or otherwise authorizing the exploitation of any Licensed Right before the end of a Holdback period and ensure that the Distributor makes the customary warranty that it will honor all such restrictions in the exercise of the Licensed Rights.

Parallel Imports (also known as "Grey Market Goods")

Parallel imports are usually hard goods which are legitimately manufactured in a country by the authorized Distributor of that Territory and then either sold by that Distributor (or more often imported by a reseller) into a country without the authorization of the owner of the intellectual property rights in the importing country. DVDs or downloaded copies that are parallel imports are not considered infringing works in many countries. Even so, a Notice and Takedown letter to any website selling the hard goods may bring some positive results. When DVD units are offered on websites like Amazon or eBay, it is helpful to identify the supplier. If it is a Distributor with which the Licensor has a business relationship, contacting that Distributor directly may be the most efficient way to resolve the parallel importation.

Country	Survey of Treatment of Parallel Imports
Australia	**Illegal** with respect to audiovisual recordings.
European Union	**Legal** between Member States (subject to the doctrine of exhaustion where the exhaustion of rights in any Member State exhausts those rights in all Member States). The rental right is not considered exhausted in the EU, so the unauthorized rental of a copy imported from one EU Member State to another EU Member State can be opposed. Illegal if from outside of the EU.
Hong Kong	**Illegal** with respect to audiovisual recordings, but not a criminal offense unless the work is imported within fifteen (15) months from the date the copyrighted work was first published anywhere in the world.
Japan	**Legal**, but audiovisual articles marketed for export from Japan are prohibited from being "re-imported" and sold domestically.
New Zealand	The Copyright Act 1994 bans the commercial parallel importation of films for five (5) months from the date the film was first released. This ban is due to expire on October 31, 2016.
United States of America	**Illegal** – with respect to "non-round trip" goods (i.e., other than goods manufactured in the U.S. with the authority of the U.S. copyright owner, exported to a foreign territory, and then imported on a "round trip" back to the U.S. by a parallel importer). With respect to round trip parallel imports, the U.S. Supreme Court found that the first sale in the United States exhausts the Licensor's distribution right, and thus it is not a violation of Section 602 of the Copyright Act of 1976 which, inter alia, gives the copyright owner the right to prohibit the unauthorized importation of copies.

Glossary of Terminology

This section is intended to provide a basic understanding of commonly used terminology. Certain definitions have been excerpted from the IFTA® International Schedule of Definitions.

The selected terms in this section may have more than one meaning and/or application in the field of computer technology and do not reflect technical explanations.

Ad Broker an entity that represents and is authorized to sell the advertising space of one or more websites.

Ad Network an aggregator of advertising inventory for many websites. Ad networks are the sales representatives for the websites within the network.

Ad Serving the delivery of ads by a server to an end user's computer on which the ads are then displayed by a browser and/or cached. Ad serving is normally performed either by a website publisher or by a third-party ad server. Ads can be embedded in the website or served separately.

App Store Notification the sending of a notice to application store operators (*e.g.*, App Store or GooglePlay) of applications available within their application store which make infringing content available to consumers so that the operator can remove the application from its store and/or block access to the application.

Attribution Procedure a procedure to verify that an authentication, display, message, record or performance is that of a particular natural person or legal entity as an Authorized Subscriber, or to detect changes or errors in information.

Authorized Subscriber any natural person or legal entity who has been verified by an attribution procedure as someone who is legally entitled to access and utilize a service.

BitTorrent a common protocol used for P2P file sharing, whereby users host and share smaller fragments of a complete file (*e.g.*, Motion Picture Copy) that are downloaded by other users and reconstructed into the complete file using a BitTorrent client.

Example: µTorrent

Cache computer memory (RAM) and disk (hard drive) used to temporarily store the most frequently requested content/files/websites in order to expedite delivery to the user. Caches can be local (*i.e.*, on a browser) or on a network.

Closed Network the interconnected facilities of a closed, private communications network which uses Internet Protocol or other secure data transmission protocol for communication among Authorized Computers (including Mobile Devices) of Authorized Subscribers connected to that Closed Network.

Cloud Computing a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Example: Apple's iCloud

Computer an electronic device that accepts and manipulates digital information or data in response to a sequence of instructions in order to view a Motion Picture Copy where the type and order of the instructions can be defined, selected and entered by the user of the Computer.

Copyright a legal term used to describe the ownership rights which creators have over their literary and artistic works that are fixed in a tangible medium of expression. Copyright covers both published and unpublished works. Copyright registration conveys a presumption of ownership and other statutory rights.

Cord Cheater(s) any natural person or legal entity that shares a subscription service password outside the parameters of the paid for subscription.

DCP (Digital Cinema Package) the digital equivalent of a film print made for playback on a Digital Cinema system. A DCP consists of a set of digital files representing pictures, sounds and data, which has been compressed, encrypted and packaged for distribution. DCP's are created following the strict guidelines set out in the Digital Cinema Initiatives (DCI).

Digital Rights Management (DRM) a sequence of software or hardware instructions embodied in, related to or activated by a Motion Picture Copy that controls or manages copying, viewing, altering, or accessing the Motion Picture, its content or elements or associated Rights Management Information.

Digital Watermarking a method of inserting an imperceptible message into media content that can be retrieved from the content even if the content has undergone a transformation (such as transforming digital content to analog and then back to digital).

DNS (Domain Name System) a distributed Internet directory service that is used mainly to translate human readable domain names into the corresponding IP addresses. In simple terms, DNS serves as a "phone book" for the Internet, but it also has many other important functions. The website http://www.dnsstuff.com provides useful tools to rights holders that discover their work illegally available on the Internet. The website is available to the public and allows users to gather preliminary information on an infringing website, such as the ISP, the server(s) location, the website's registrar agency and registrant.

Domain Name a name that identifies a website registered on the Internet. These normally appear as component of a website's URL. Commonly, domain names act as hostnames to provide more memorable names to stand in for numeric IP addresses.

Example: ifta-online.org

Download to make available a digital Motion Picture Copy on the Internet or a Closed Network in a manner that allows its transmission to a Computer or Mobile Device for making another exact digital Copy on such Computer or Mobile Device and retaining such copy for use for more than a transient period of time on such Computer or Mobile Device after completion of the initial continuous period of transmission.

Encryption the process of encoding an asset in such a way that only authorized parties may access it by using a digital encryption key.

Evidence Gathering assembling evidence of infringement, such as the IP address, the ISP, and the location of the infringing content, obtained through monitoring so that the rights owner can make informed decisions regarding their legal options.

Fingerprinting a coded string of binary digits within the metadata of an asset that uniquely identifies the asset.

Firewall security measures that control incoming and outgoing traffic to a networked computer system.

Forensic Watermarking watermarking technique used to allow content owners to trace and source particular copies of content.

Geofiltering (aka "geoblocking") technology that restricts access to content and limits distribution to users within the licensed Territory or region. Two modes of determining the location of the user trying to access the content are typically involved: 1) the billing address of the credit card used to purchase the content and 2) the location of the IP address used to access the content.

Graduated Response (aka "three strikes") requirements on ISPs to cooperate with rights holders and government in responding to illegal file-sharing. Typically, a governing authority or local organization may be empowered to act as a clearing house for notices, such as with HADOPI in France. Notices are sent by the ISPs to its subscribers engaging in infringing activity with escalating messages for repeat infringers with a mitigation measure imposed on subscribers who do not cease such infringing activity after multiple warnings. Graduated response systems can be statutory or voluntary.

"Hard Goods" Piracy physical piracy of copyrighted works contained in DVDs and video cassettes.

Injunction (aka "injunctive relief") a judicial order which requires a party to refrain from doing something which would violate the legal right of another party, or requiring the party to carry out a certain act to avoid or as restitution for a violation of a party's rights.

Example: a court order against operators of a BitTorrent website requiring that they refrain from hosting, linking to, distributing, reproducing, performing, selling, offering for sale, making available for download, streaming or making any other use of any copy or copies of a particular film.

Internet the interconnected facilities of a publicly available communications network which uses Internet Protocol for data transmission to Computers (including Mobile Devices) connected to that network. Also referred to as the "web" or "online" environment.

Internet Service Provider (ISP) a company that provides access to the Internet. Access ISPs directly connect customers to the Internet using copper wires, wireless or fiber-optic connections. Hosting ISPs lease server space for smaller businesses and host other people's servers (colocation). Transit ISPs provide large tubes for connecting *hosting ISPs* to *access ISPs*. ISPs employ a range of technologies to enable consumers to connect to their network, including dial up, DSL (typically Asymmetric Digital Subscriber Line, ADSL), broadband wireless, cable modem, fiber to the premises (FTTH), and Integrated Services Digital Network (ISDN).

Example: AT&T, Cablevision, Comcast, Time Warner Cable

ISP Notification (in U.S. sometimes referred to as "DMCA Notice") sending notices of infringing content located on an ISP's server to that ISP so that the ISP can either remove the infringing content or forward the notice on to their subscriber in order to comply with the relevant local laws.

Internet Protocol (IP) the Transmission Control Protocol (TCP) and Internet Protocol (IP) or successors or substantially similar substitute protocols.

Investigative Services services which provide threat analysis, incident response, and/or tracing the source of piracy leaks.

IP Address a computer's unique address that computers within a network use to identify and communicate with one another. Each computer connected to the Internet has an IP Address so that information can be delivered to the requesting computer.

Example: 72.14.207.100

KDM (Key Delivery Message) with respect to Digital Cinema, a KDM refers to the encrypted key to unlock the content as well as the certificate and a signature for verification purposes.

Metadata information that describes a certain set of other data.

Mobile Device a portable Computer, a substantial purpose of which is facilitating telephonic communication, but which also incorporates functionality that allows viewing of a Motion Picture Copy.

Monetization of Unauthorized Uses as Revenue Enhancement identification software and advertising tools used by certain websites and intermediary services to enable Licensors to generate additional revenue streams and a wider audience base from content which is distributed online without the Licensor's authority.

Example: YouTube Content ID

Name Server a server which implements a network service by providing responses to queries against the directory service by translating a domain name into an IP address.

Non-disclosure Agreement (NDA) a contract in which the parties formally agree to treat as confidential certain disclosed information and to refrain from disclosing such information without authorization.

Online Monitoring automated systems (utilizing "surfs" or "spiders") that monitor websites, P2P file sharing networks, cyberlockers, chat sites, and various other places to determine whether assets are being distributed illegally on the Internet. Some online monitoring vendors may employ technology that can reach back to identify past infringement of a particular asset.

Online Service Provider (OSP) a generic term that describes any company, organization or group that provides an online service. These types of services may include websites, discussion forums, chat rooms, or web mail. OSPs may also refer to a company that provides dial-up access to the Internet.

Example: YouTube, Facebook, Twitter

Payment Processor Notification notification to a payment processor that their systems are being used to process or facilitate sales transactions of copyright-infringing products and/or counterfeit trademark products.

Peer-to-Peer (P2P) file sharing technology that enables multiple users to access and share digital files without having those files stored in a central database. P2P software connects a computer to other computers running the same software – sometimes giving access to millions of computers at a time – often used to share digital files.

Examples of P2P networks: µTorrent, Deluge, iLivid and Tixati

Playback Control Watermarking watermarking technique used to control the type of player (e.g., professional projectors, Blu-ray Players, etc.) that can play and/or copy the file.

Example: Verance/Cinavia

Registrar a company accredited by the Internet Corporation for Assigned Names and Numbers (ICANN), or some other national authority, to register Internet Domain Names.

Example: Network Solutions, LLC, GoDaddy.com, Inc.

Registrant the entity that registers the domain name.

Search Engine a service that matches a search term input by a user with corresponding indexed website content provided as "search results."

Examples: Google, Yahoo! Ask.com, LexisNexis (private, fee-based), Grokster (P2P service).

Search Engine Notification - sending notices of infringing websites to search engine providers (*e.g.*, Google and Yahoo!) so that the provider can remove the infringing site from its search algorithm or its results in accordance with relevant local laws or voluntarily.

Security Plan specific measures to limit access to and secure copyrighted materials for all phases of production and distribution.

Server a computer which manages and provides access to a centralized resource or service in a network.

Stream to make available a Motion Picture Copy on the Internet or a ClosedNet in a manner that allows continuous viewing of the Motion Picture Copy in substantially linear form on a Computer or Mobile Device simultaneously with the transmission of such Motion Picture Copy over the Internet or Closed Network but which does not allow making another digital copy except for a transient period of time necessary to facilitate such viewing.

URL (Uniform Resource Locator) the address for a specific website. It contains unique information about the server and the path on the server to find and retrieve information requested by the user.

Example: http://www.ifta-online.org

URL Redirection (aka "URL forwarding") a technique used to make a website available under more than one URL address.

USB (Universal Serial Bus) an industry standard interface for connecting peripheral devices to a computer, including flash drives, external hard drives, cameras, and mobile devices.

VPN (Virtual Private Network) a private data network that uses the Internet to transfer information using secure methods. In essence a VPN changes or masks a user's IP address to make it appear as though the user is accessing the Internet from another location. VPNs are sometimes used by "cord cheaters" or subscribers to access content outside the scope of a paid for subscription.

Web see Internet

Web Browser a software application that accesses and allows users to interact with web pages on the World Wide Web or a local area network. The browser is a program that sends requests to web servers, receives and interprets the corresponding files and displays the information on the computer screen.

Example: Internet Explorer, Firefox, Safari, Chrome

Web Host a type of Internet hosting service that allows users to make their websites accessible on the Internet. Web Hosts are companies that provide space on computer servers they own to provide a variety of services to users, including e-mail hosting, data center space, etc.

Examples: 1and1.com, GoDaddy, Network Solutions, HostMonster, HostGator, BlueHost

Website (aka "site") a set of interconnected data resources at an addressable location on the Internet or a Closed Network which is accessible by other users or Authorized Subscribers of the applicable network. Websites may also be referred to as OSPs or ISPs in connection with its legal obligations to remove infringing material on its website.

Website-blocking (aka "site blocking") refers to a court ordered injunction requiring an ISP to restrict or block access of the ISP's users to a certain website(s) that provides infringing material. Forms of website-blocking include, DNS blocking and IP address blocking.

Note: Site blocking refers to an ISP blocking its subscribers' access to a certain website. Although site blocking may not be available in certain territories, it may be possible to get other forms of injunctive relief against infringing websites.

Wireless System a closed system of integrated telecommunications facilities that allow system Subscribers to access an over-the-air digital signal.

WHOIS Database a publicly accessible database that maintains domain name owners' contact information, such as names, addresses, email addresses, etc.